UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

EDWARD MARSHALL, individually and on behalf of all others similarly situated, Plaintiff, v. PROGRESS SOFTWARE CORPORATION; PENSION BENEFIT INFORMATION, LLC d/b/a PBI RESEARCH SERVICES; and TEACHERS INSURANCE AND ANNUITY ASSOCIATION OF AMERICA Defendants.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Edward Marshall ("Plaintiff") brings this action against Progress Software Corporation ("PSC"), Pension Benefit Information, LLC d/b/a PBI Research Services ("PBI"), and Teachers Insurance and Annuity Association of America ("TIAA") (collectively, "Defendants"), individually and on behalf of all others similarly situated ("Class Members"), and alleges upon personal knowledge as to their own actions and their counsel's investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard personally identifiable information ("PII" or "Private Information") including, but not limited to, Plaintiff's and Class Members' names, Social Security numbers, birthdates, gender, address, demographic information, insurance policy numbers, and other financial information.

2. Defendant PSC is a Massachusetts based software company that offers a wide range of software products and services to corporate and governmental entities throughout the United States and the world, including cloud hosting and secure file transfer services such as MOVEit.

3. Defendant PBI is a Minnesota based company that provides audit and search services to pension funds, insurance companies, and others. PBI uses Defendant PSC's MOVEit file transfer services for this purpose, including the transfer of individuals' PII.

4. Defendant TIAA is a New York based company that provides insurance and financial services to individuals, agents, and businesses. TIAA contracted with PBI to obtain audit and/or research services.

5. Defendants possessed and controlled Plaintiff's PII because Plaintiff inherited a TIAA retirement account from his deceased spouse. TIAA provided Plaintiff's PII to PBI along with the PII of many other TIAA customers and agents.

6. PBI succinctly summarizes the breach in a letter it sent to Plaintiff: "On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review."[1]

[1] A copy of the Data Breach Notice Plaintiff received is attached hereto as Exhibit 1.

7. According to PBI, "Our investigation determined that the following types of information related to you were present in the server at the time of the event: name, Social Security number, gender, date of birth, and address."[2]

8. During its business operations, Defendants acquired, collected, utilized, and derived a benefit from Plaintiff's and Class Members' Private Information. Therefore, Defendants owed and otherwise assumed statutory, regulatory, contractual, and common law duties and obligations, including to keep Plaintiff's and Class Members' Private Information confidential, safe, secure, and protected from the type of unauthorized access, disclosure, and theft that occurred in the Data Breach described below.

9. Despite its duties to Plaintiff and Class Members related to and arising from its cloud hosting and secure file transfer services and applications involving MOVEit, PSC stored, maintained, and/or hosted Plaintiff's and Class Members' Private Information on its MOVEit transfer services software that was negligently and/or recklessly configured and maintained so as to contain security vulnerabilities that resulted in multiple breaches of its network and systems or of its customers' networks and systems. These security vulnerabilities existed as far back as 2021. As a result of the breach, unauthorized third-party cybercriminals gained access to and obtained Plaintiff's and Class Members' PII.

10. On or about May 31, 2023, PSC posted a notice on its website stating that it had found an SQL injection vulnerability in its MOVEit Transfer application dating as far back as 2021 that allowed an unauthorized third party to access Plaintiff's and Class Member's Private Information (the "Data Breach").[3]

---

[2] *Id*.

[3] *MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)*, Progress Community,

11. Plaintiff brings this class action lawsuit on behalf of himself and those similarly situated to address Defendants' inadequate safeguarding of Class Members' Private Information that they collected and maintained; for failing to provide adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown criminal third party; and for failing to timely identify precisely what specific type of information was accessed.

12. Upon information and belief, Defendants maintained the Private Information of millions of individuals in a negligent manner. In particular, the Private Information was maintained on computer systems and networks that utilized MOVEit, which contained security vulnerabilities. These security vulnerabilities led to dozens of cyberattacks, including the cyberattack that resulted in the theft of Plaintiff's PII.

13. Upon information and belief, PBI negligently chose to utilize PSC's MOVEit software to store and transfer Plaintiff's and Class Members' PII despite the fact that MOVEit contained security vulnerabilities.

14. Upon information and belief, TIAA negligently chose to utilize PBI's search services with Plaintiff's and Class Members' PII despite the fact that MOVEit contained security vulnerabilities.

15. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendants because other file transfer programs had previously been subjected to criminal hacking, and thus Defendants were on notice that failing to take appropriate design and protective

---

https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023 (last visited June 22, 2023); *see also* Sean Lyngaas, *Exclusive: US Government Agencies Hit in Global Cyberattack*, CNN (June 15, 2023), https://www.cnn.com/2023/06/15/politics/us-government-hit-cybeattack/index.html.

measures would expose and increase the risk that the Private Information could be compromised and stolen.

16. The cyberattack at issue was carried out by the well-known Russian cybergang, Clop.

17. Hackers such as Clop can and do offer for sale unencrypted, unredacted Private Information to criminals. The exposed Private Information of Plaintiff and Class Members can, and likely will, be sold repeatedly on the dark web.

18. Plaintiff and Class Members now face a current and ongoing risk of identity theft, which is heightened here by the loss of Social Security numbers – the gold prize for identity thieves.

19. Upon information and belief, this Private Information was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect the Private Information of Plaintiff and Class Members.

20. When PSC's customers use MOVEit Transfer application, they entrust PSC with their confidential files and information, including Plaintiff and Class Members' Private Information, and PSC accepts responsibility for securely maintaining such Private Information.

21. When PBI's customers use its services, they entrust PBI with their confidential files and information, including Plaintiff and Class Members' Private Information, and PBI accepts responsibility for securely maintaining such Private Information.

22. When TIAA's customers use its services, they entrust TIAA with their confidential files and information, including Plaintiff and Class Members' Private Information, and TIAA accepts responsibility for securely maintaining such Private Information.

23. Defendants have not made any assurances that they have adequately enhanced their data security practices to sufficiently safeguard from a similar vulnerability in the MOVEit Transfer Application in the future.

24. While many details of the Data Breach remain in the exclusive control of Defendants, upon information and belief, Defendants breached their duties and obligations by failing, in one or more of the following ways: (i) failing to design, implement, monitor, and maintain reasonable software and/or network safeguards against foreseeable threats; (ii) failing to design, implement, and maintain reasonable data retention policies; (iii) failing to adequately train staff on data security; (iv) failing to comply with industry-standard data security practices; (v) failing to warn Plaintiff and Class Members of Defendants' inadequate data security practices; (vi) failing to encrypt or adequately encrypt the Private Information; (vii) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (viii) failing to utilize widely available software able to detect and prevent this type of attack, and (ix) otherwise failing to secure the software and hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

25. As a result of Defendants' unreasonable and inadequate data security practices that resulted in the Data Breach, Plaintiff and Class Members are at a current and ongoing risk of identity theft and have suffered numerous actual and concrete injuries and damages, including: (i) invasion of privacy; (ii) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (iii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iv) financial "out of pocket" costs incurred due to actual identity theft; (v) loss of time incurred due to actual identity theft; (vi) loss of time due to increased spam and targeted marketing emails; (vii) diminution of value of their

Private Information; (viii) anxiety, annoyance, and nuisance; and (ix) the continued risk to their Private Information, which remains in the control of Defendants, and which is subject to further breaches, as long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

26. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, future costs of identity theft monitoring, injunctive relief including improvements to Defendants' data security systems, and future annual audits.

27. Accordingly, Plaintiff brings this action against Defendants seeking redress for their unlawful conduct and asserting claims for: (i) negligence; (ii) breach of third-party beneficiary contract; (iii) negligence per se; (iv) unjust enrichment; (v) declaratory judgment; and violation New York General Business Law § 349.

PARTIES

28. Plaintiff Edward Marshall is, and at all times mentioned herein was, an individual citizen of the State of Connecticut.

29. Defendant Progress Software Corporation is a for profit corporation organized under the laws of the State of Delaware with its principal place of business located at 15 Wayside Road, Suite 4, Burlington, Massachusetts 01803. Service of process is proper on Corporation Service Company as agent located at 84 State Street, Boston, Massachusetts 02109.

30. Defendant Pension Benefit Information, LLC d/b/a PBI Research Services is a for profit limited liability company organized under the laws of the State of Delaware with its principal place of business located at 333 South 7th Street, Suite 2400, Minneapolis, Minnesota 55402.

Service of process is proper on Corporation Service Company as agent located at 251 Little Falls Drive, Wilmington, Delaware 19808.

31. Defendant Teachers Insurance and Annuity Association of America is domiciled and maintains its principal place of business in the State of New York.

JURISDICTION AND VENUE

32. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members exceeds 100, many of whom, including Plaintiff, have different citizenship from Defendants. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

33. This Court has personal jurisdiction over Defendants because they conduct substantial business in this jurisdiction and because Plaintiff's claims arise out of or relate to Defendants' contacts with, and conduct within, this District. Further, this Court has general jurisdiction over Defendant TIAA because its corporate headquarters is located in this District.

34. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant TIAA is based in this District, Defendant PSC marketed, sold, and maintained the MOVEit transfer application in this District, and the harm caused to Plaintiff and Class Members emanated from this District.

FACTUAL ALLEGATIONS

PSC's Business

35. PSC, which is based in Burlington, Massachusetts, is a software company that offers a wide range of products and services to government agencies and corporate entities across the United States and around the world, including MOVEit.

36. MOVEit is a "[m]anaged File Transfer and automation software that guarantees the security of sensitive files both at-rest and in-transit, ensures reliable business processes and addresses data security compliance requirements.[4]

37. As a condition of receiving secure file transfer services, PSC requires that its government and corporate customers entrust it and its MOVEit transfer software application with highly sensitive Private Information belonging to Plaintiff and Class Members.

38. Because of the highly sensitive nature of the Private Information that PSC acquires, maintains, and transfers, PSC "guarantees the security of sensitive files,"[5] and promises, among other things, to: keep customers' files private; comply with industry standards related to data security and maintenance of its customers' files and the Private Information contained therein; only disclose the sensitive information for business purposes and reasons related to the services it provides; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

39. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' Private Information, PSC assumed legal and equitable duties and knew or should have known that it was responsible for ensuring the security of Plaintiff's and Class Members' Private Information to protect it from unauthorized disclosure and exfiltration.

[4] *Progress Brochure*, available at https://d117h1jjiq768j.cloudfront.net/docs/default-source/default-document-library/progress-corporate-brochure-2023-rgb.pdf?sfvrsn=a0b1f671_3 (last visited June 22, 2023).
[5] *Id.*

40. Plaintiff and Class Members relied on PSC to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this information, which PSC failed to do.

PBI's Business

41. PBI, which is based in Minneapolis, Minnesota, is a company that provides auditing and research services to pension funds, insurance companies, and others. PBI uses MOVEit file transfer services for this purpose, including the transfer of individuals' PII.

42. As a condition of performing its search services, PBI requires that its government and corporate customers entrust it with highly sensitive Private Information belonging to Plaintiff and Class Members.

43. Because of the highly sensitive nature of the Private Information that PBI acquires, maintains on its network, and inputs into PSC's MOVEit file transfer software, PBI states that "[p]rotecting and securing the information of our clients and our company is of critical importance to PBI,"[6] and promises, among other things, to: keep customers' files private; comply with industry standards related to data security and maintenance of its customers' files and the Private Information contained therein; only disclose the sensitive information for business purposes and reasons related to the services it provides; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

44. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' Private Information, PBI assumed legal and equitable duties and knew or should have known that it was responsible for ensuring the security of Plaintiff's and Class Members' Private Information to protect it from unauthorized disclosure and exfiltration.

[6] https://www.pbinfo.com/data-security/

45. Plaintiff and Class Members relied on PBI to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this information, which PBI failed to do.

TIAA's Business

46. TIAA, which is based in New York, is a company that provides financial, insurance, and annuity services to individuals, agents, and businesses. TIAA contracted with PBI to provide auditing and research services.

47. As a condition of providing its insurance and annuity services, TIAA requires that customers, agents, and businesses entrust it with highly sensitive Private Information belonging to Plaintiff and Class Members.

48. Because of the highly sensitive nature of the Private Information that TIAA acquires, maintains on its network, and provides to third parties, including PSC and PBI, TIAA provides assurances to customers, agents, and businesses that it keeps their Private Information secure:

> We protect your personal information. TIAA's Security Operations Center provides fast, accurate, thorough and non-stop protection from cyber attacks. Stringent security patching practices address vulnerabilities that attackers try to exploit. Data loss prevention controls help ensure data doesn't fall into the wrong hands. Award-winning security awareness training drives a culture of accountability for customer data protection Robust supplier risk management practices help ensure our suppliers adhere to our expectations.[7]

49. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' Private Information, TIAA assumed legal and equitable duties and knew or should have

[7] https://www.tiaa.org/public/support/security-center (last visited Aug. 29, 2023)

known that it was responsible for ensuring the security of Plaintiff's and Class Members' Private Information to protect it from unauthorized disclosure and exfiltration.

50. Plaintiff and Class Members relied on TIAA to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this information, which TIAA failed to do.

The Data Breach

51. On May 31, 2023, PSC reported a vulnerability in MOVEit Transfer and MOVEit Cloud (CVE-2023-34362) that could lead to escalated privileges and potential unauthorized access to the environment. Progress purportedly launched an investigation, alerted MOVEit customers of the issue and provided mitigation steps.[8]

52. PSC applied additional patches on June 9 and June 16 to purportedly address other vulnerabilities that were discovered.[9]

53. The Russian cyber gang Clop took responsibility for the attack—which began on May 27, 2023—and began attempts to ransom and exploit data accessed from MOVEit.[10]

54. PBI was one of the companies whose data was accessed and stolen, which included PII of millions of individuals, including Plaintiff and Class Members.

55. PBI, as a provider of search services, obtained data of Plaintiff and Class Members from businesses utilizing PBI's search services, including TIAA.

56. PBI began informing its clients, including TIAA, of the Data Breach on or around June 16, 2023.

[8] https://www.progress.com/security/moveit-transfer-and-moveit-cloud-vulnerability
[9] *Id.*
[10] https://www.bleepingcomputer.com/news/security/clop-ransomware-gang-starts-extorting-moveit-data-theft-victims/

57. PBI's clients, including TIAA, also publicly acknowledged that PII of millions of individuals had been accessed in the Data Breach.

58. Defendants negligently maintained Plaintiff's and Class Members' Private Information, which allowed unauthorized cybercriminals to access and exfiltrate the Private Information through the Data Breach, including, but not limited to, Social Security numbers, financial information, and driver's licenses.

59. Defendants had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep Plaintiff and Class Members' Private Information confidential and to protect them from unauthorized access and disclosure.

60. Plaintiff and Class Members permitted their Private Information to be provided to Defendants with the reasonable expectation and understanding that Defendants would comply with its obligations to keep said Private Information confidential and secure from unauthorized access and timely notify Class Members of any security breaches.

61. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks in recent years, including recent similar attacks against secure file transfer companies such as Accellion and Fortra by the same Russian cyber gang, Clop.[11]

62. Therefore, because of the type of data and Private Information maintained, Defendants knew or should have known that their systems and the records would be targeted by cybercriminals.

Plaintiff Edward Marshall's Experience

[11] *See* Bill Toulas, *Fortra Shares Findings on GoAnywher MFT Zero-Day Attacks*, BleepingComputer (Apr. 19, 2023), https://www.bleepingcomputer.com/news/security/fortra-shares-findings-on-goanywhere-mft-zero-day-attacks/; *see also* Ionut Ilascu, *Global Accellion Data Breaches Linked to Clop Ransomware Gang*, BleepingComputer (Feb. 22, 2021), https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/.

63. Plaintiff is a TIAA customer, having inherited a retirement account from his deceased spouse who worked as a teacher prior to her passing.

64. Plaintiff is very careful about sharing his sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

65. Plaintiff stores any documents containing his sensitive Private Information in a safe and secure location or destroys such documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts in an effort to safeguard and protect his PII.

66. On approximately August 11, 2023, Plaintiff received letter from PBI notifying him that his PII had been compromised in the Data Breach. *See* Exhibit 1.

67. As a result of the Data Breach, Plaintiff has and will continue to spend time trying to mitigate the consequences of the Data Breach. This includes time spent verifying the legitimacy of communications related to the Data Breach, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

68. The harm caused to Plaintiff cannot be undone.

69. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

70. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

71. Plaintiff has suffered imminent and impending injury arising from the present and

ongoing risk of fraud, identity theft, and misuse resulting from their Private Information being placed in the hands of cybercriminals.

72. Future identity theft monitoring is reasonable and necessary and such services will include future costs and expenses.

73. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendants' control, is protected, and safeguarded from future breaches.

The Data Breach Was Foreseeable

74. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members because of a breach.

75. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on their network, amounting to potentially millions of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

76. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[12]

77. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches preceding the date of the breach.

[12] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed June 22, 2023).

78. In 2022, 1,774 data breaches occurred, affecting approximately 392,000,000 victims.[13]

79. In light of the recent high profile cybersecurity incidents at other file transfer and storage companies, including Accellion and Fortra, Defendants knew or should have known that its electronic records would be targeted by cybercriminals.

80. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.[14]

81. Therefore, the increase in such attacks, and the attendant risk of future attacks, were widely known to the public and to anyone in Defendants' industry, including Defendants.

Value of PII

82. Individuals' PII remains of high value to criminals, as evidenced by the prices offered through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[15] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an

[13] *See* 2022 Data Breach Annual Report, available at https://www.idtheftcenter.org/publication/2022-data-breach-report/

[14] FBI, Secret Service Warn of Targeted, Law360 (Nov.18,2019), https://www.law360.com/articles/1220974/fbisecret-service-warn-of-targeted-ransomware.

[15] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/. (last accessed June 22, 2023).

average market value of $120.[16] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[17]

83. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts.

84. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information…[is] worth more than 10x on the black market."[18]

85. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

86. The fraudulent activity resulting from the Data Breach may not come to light for years.

87. There is also a robust legitimate market for the type of sensitive information at issue here. Marketing firms utilize personal information to target potential customers, and an entire economy exists related to the value of personal data.

88. Moreover, there may be a time lag between when harm occurs versus when it is discovered and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may

[16] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, available at: https://www.privacyaffairs.com/dark-web-price-index-2021/ (last accessed June. 22, 2023).
[17] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.
[18] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed June. 22, 2023).

> continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[19]

89. As such, future monitoring of financial and personal records is reasonable and necessary.

Defendants Failed to Properly Protect Plaintiff's and Class Members' Private Information

90. Defendants could have prevented this Data Breach by properly testing, monitoring, auditing, securing and encrypting the systems containing the Private Information of Plaintiff and Class Members.

91. Defendants' negligence in not safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendants to protect and secure sensitive data they maintain.

92. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

93. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[20]

---

[19] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed June 22, 2023).

[20] *See generally Fighting Identity Theft With the Red Flags Rule: A How-To Guide for Business*, FED. TRADE COMM., https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business (last accessed June 22, 2023).

94. The ramifications of Defendants' failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

95. To prevent and detect unauthorized cyber-attacks, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent

programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[21]

96. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….
- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….
- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….
- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact

[21] *Id.* at 3-4.

information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[22]

97. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts

[22] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at https://www.cisa.gov/news-events/news/protecting-against-ransomware (last accessed June 23, 2023).

- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications][23]

98. Moreover, given that Defendants were maintaining the PII of Plaintiff and Class Members, Defendants could and should have implemented all the above measures to prevent and detect cyberattacks.

99. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of Plaintiff and Class Members.

100. Because Defendants failed to properly protect and safeguard Plaintiff's and Class Members' Private Information, an unauthorized criminal third party was able to access Defendants' network, and access Defendants' database and system configuration files and exfiltrate that data.

Defendants Failed to Comply with FTC Guidelines

101. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

102. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide

[23] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last accessed June 22, 2023).

for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[24]

103. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

104. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

105. Defendants failed to properly implement basic data security practices.

106. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

107. Defendants were always fully aware of its obligation to protect the Private Information of Plaintiff and Class Members. Defendants were also aware of the significant

[24] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed June 22, 2023).

repercussions that would result from its failure to do so.

Defendants Failed to Comply with Industry Standards for Data Security

108. In light of the numerous high-profile data breaches targeting companies like Target, Neiman Marcus, eBay, Anthem, Deloitte, Equifax, Marriott, T-Mobile, and Capital One, Defendants were, or reasonably should have been, aware of the importance of safeguarding PII, as well as of the foreseeable consequences of its systems being breached.

109. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for PII;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

110. The FTC publishes guides for businesses for cybersecurity[25] and protection of PII[26] which includes basic security standards applicable to all types of businesses.

111. The FTC recommends that businesses:

[25] Start with Security: A Guide for Business, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf. (last accessed June 23, 2023).

[26] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed June 22, 2023).

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hacker attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

112. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as

an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[27]

113. Because Defendants were entrusted with PII, they had, and have, a duty to keep the PII secure.

114. Plaintiff and Class Members reasonably expect that when their PII is provided to a sophisticated business for a specific purpose, that business will safeguard their PII and use it only for that purpose.

115. Nonetheless, Defendants failed to prevent the Data Breach. Had Defendants properly maintained and adequately protected its systems, it could have prevented the Data Breach.

116. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

117. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

[27] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

118. The foregoing frameworks are existing and applicable industry standards in the software and data management/transfer industry, and Defendants failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

119. Upon information and belief, Defendants failed to comply with one or more of the foregoing industry standards.

Defendants' Negligent Acts and Breaches

120. Defendants participated and controlled the process of gathering the Private Information from Plaintiff and Class Members.

121. Defendants therefore assumed and otherwise owed duties and obligations to Plaintiff and Class Members to take reasonable measures to protect the information, including the duty of oversight, training, instruction, and testing of the data security policies and network systems. Defendants breached these obligations to Plaintiff and Class Members and/or was otherwise negligent because it failed to properly implement data security systems and policies for its network that would adequately safeguarded Plaintiff's and Class Members' Private Information. Upon information and belief, Defendants' unlawful conduct included, but is not limited to, one or more of the following acts and/or omissions:

a. Failing to design and maintain an adequate data security system to reduce the risk of data breaches and protect Plaintiff's and Class Members Private Information;

b. Failing to properly monitor its data security systems for data security vulnerabilities and risk;

c. Failing to audit, test and assess the adequacy of its data security system;

d. Failing to develop adequate training programs related to the proper handling of emails and email security practices;

e. Failing to put into develop and place uniform procedures and data security protections for its network;

f. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;

g. Failing to ensure or otherwise require that it was compliant with FTC guidelines for cybersecurity;

h. Failing to ensure or otherwise require that it was adhering to one or more of industry standards for cybersecurity discussed above;

i. Failing to implement or update antivirus and malware protection software in need of security updating;

j. Failing to require encryption or adequate encryption on its data systems;

k. Otherwise negligently and unlawfully failing to safeguard Plaintiff's and Class Members' Private Information provided to Defendants, which in turn allowed cyberthieves to access its IT systems.

COMMON INJURIES & DAMAGES

122. As result of Defendants' ineffective and inadequate data security practices, Plaintiff and Class Members now face a present and ongoing risk of fraud and identity theft.

123. Due to the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (iii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iv) "out of pocket" costs incurred due to actual identity theft; (v) loss of time incurred due to actual identity theft; (vi) loss of time due to increased spam and targeted marketing emails; (vii) diminution of value of their Private Information; and (viii) the continued risk to their Private Information, which remains in Defendants' control, and which is subject to further breaches, so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and

Class Members' Private Information.

The Risk of Identity Theft to Plaintiff and Class Members Is Present and Ongoing

124. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

125. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

126. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

127. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[28] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web

[28] *What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/. (last accessed June 22, 2023).

users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[29] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

128. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal information like the PII at issue here.[30] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[31] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[32]

129. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your

[29] *Id.*
[30] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web/ (last accessed June 22, 2023).
[31] *Id.; What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/. (last accessed June 22, 2023).
[32] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web (last accessed June 22, 2023).

> name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[33]

130. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.[34]

131. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[35]

132. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. And the Social Security Administration has warned that identity

[33] Social Security Administration, *Identity Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf. (last accessed June 22, 2023).
[34] *See id.*
[35] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited June 22, 2023).

thieves can use an individual's Social Security number to apply for additional credit lines.[36]

133. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[37]

134. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[38] Defendants did not rapidly report to Plaintiff and the Class that their Private Information had been stolen.

135. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

136. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

137. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

---

[36] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited June 22, 2023).
[37] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last accessed June 22, 2023).
[38] *Id.*

138. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[39]

139. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (i) encrypting information stored on computer networks; (ii) retaining payment card information only as long as necessary; (iii) properly disposing of personal information that is no longer needed; (iv) limiting administrative access to business systems; (v) using industry-tested and accepted methods for securing data; (vi) monitoring activity on networks to uncover unapproved activity; (vii) verifying that privacy and security features function properly; (viii) testing for common vulnerabilities; and (ix) updating and patching third-party software.[40]

140. Defendants' failure to properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Loss of Time to Mitigate the Risk of Identify Theft and Fraud

141. As a result of the recognized risk of identity theft, when a Data Breach occurs, and

[39] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last accessed June 22, 2023).
[40] *See generally* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last accessed June 22, 2023).

an individual is notified by a company that their Private Information was compromised, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

142. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

143. These mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[41]

144. These mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[42]

[41] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf. (last accessed June 22, 2023).
[42] *See* Federal Trade Commission, Identity Theft.gov, https://www.identitytheft.gov/Steps (last accessed June 22, 2023).

145. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[43] Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[44]

Diminution of Value of the Private Information

146. PII is a valuable property right.[45] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

147. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[46] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[47,]

[43] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last accessed June 22, 2023). ("GAO Report").
[44] *See* https://www.identitytheft.gov/Steps (last accessed June 22, 2023).
[45] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted) (last accessed June 22, 2023).
[46] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed June 22, 2023).
[47] https://datacoup.com/. (last accessed June 22, 2023).

Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[48]

148. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the Dark Web, where it may soon be available and holds significant value for the threat actors.

Future Cost of Credit and Identify Theft Monitoring Is Reasonable and Necessary

149. To date, Defendants have done nothing to provide Plaintiff and Class Members with relief for the damages they have suffered because of the Data Breach despite Plaintiff and Class Members being at risk of identity theft and fraud for the foreseeable future.

150. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information (e.g. social security numbers), and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes – e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

151. It must be noted there may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be

[48] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html. (last accessed June 22, 2023).

> held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at 29.

152. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that their Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

153. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[49] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

154. Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for their entire lives.

155. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach. This is a recurring future cost that Plaintiff and Class Members would not need to bear but for Defendants' failure to safeguard their Private Information.

[49] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1. (last accessed June 22, 2023).

Injunctive Relief Is Necessary to Protect Against Future Data Breaches

156. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the control of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

CLASS ACTION ALLEGATIONS

157. Plaintiff brings this nationwide class action on behalf of himself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

158. The "Nationwide Class" that Plaintiff seeks to represent is defined as follows:

> All persons whose Private Information was accessed or acquired during the Data Breach as a result of the exploitation of Progress Software Corporation's MOVEit Application vulnerability (the "Class").

With a "PBI Subclass" defined as follows:

> All persons whose Private Information was maintained by PBI and accessed or acquired during the Data Breach as a result of the exploitation of Progress Software Corporation's MOVEit Application vulnerability (the "PBI Subclass").

With a "TIAA Subclass" defined as follows:

> All persons whose Private Information was maintained by TIAA and accessed or acquired during the Data Breach as a result of the exploitation of Progress Software Corporation's MOVEit Application vulnerability (the "TIAA Subclass").

159. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants has a controlling interest; all individuals who make a timely election to be excluded

from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

160. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

161. Numerosity, Fed. R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are millions of individuals whose Private Information may have been improperly accessed in the Data Breach, and the Class is readily identifiable within Defendants' records.

162. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendants had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendants had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendants had duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the Private Information of Plaintiff and Class Members;

e. Whether and when Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendants' wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

163. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendants' misfeasance.

164. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was maintained and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

165. Adequacy of Representation, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class.

Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

166. Superiority, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

167. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary

and duplicative of this litigation.

168. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, including its privacy policy, uniform methods of data collection, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

169. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

170. Unless a Class-wide injunction is issued, Defendants may continue in its failure to properly secure the Private Information of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Petition.

171. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

172. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in obtaining, storing, collecting, maintaining, using, and/or safeguarding their Private Information;

b. Whether Defendants breached a legal duty to Plaintiff and Class Members to exercise due care in obtaining, storing, collecting, maintaining, using, and/or safeguarding their Private Information;

c. Whether Defendants failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendants adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

e. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

f. Whether Defendants' data security practices related to its MOVEit Application prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether Defendants' data security practices related to its MOVEit Application prior to and during the Data Breach were consistent with industry standards;

h. Whether hackers obtained Class Members' Private Information via the Data Breach;

i. Whether Defendants breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members; and

j. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members Against All Defendants)

173. Plaintiff and the Class repeat and re-allege each and every allegation as if fully set forth herein.

174. Defendants knowingly collected, acquired, stored, and/or maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting the Private Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

175. The duty included obligations to take reasonable steps to prevent disclosure of the Private Information, and to safeguard the information from theft. Defendants' duties included the

responsibility to design, implement, and monitor data security systems, policies, and processes to protect against reasonably foreseeable data breaches such as this Data Breach.

176. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, policies, and procedures, and the personnel responsible for them, adequately protected the Private Information.

177. Defendants owed a duty of care to safeguard the Private Information due to the foreseeable risk of a data breach and the severe consequences that would result from its failure to so safeguard the Private Information.

178. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and those individuals who entrusted them with their PII, which is recognized by laws and regulations including but not limited the FTC Act, as well as common law. Defendants was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

179. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

180. Defendants' duty to use reasonable care in protecting Private Information arose not only as a result of the statutes and regulations described above, but also because Defendants is bound by industry standards to protect Private Information that it either acquires, maintains, or stores.

181. Defendants breached their duties, and thus were negligent, by failing to use

reasonable measures to protect Plaintiff's and Class Members' Private Information, as alleged and discussed above.

182. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the data transfer and storage industry.

183. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

184. The imposition of a duty of care on Defendants to safeguard the Private Information they maintained is appropriate because any social utility of Defendants' conduct is outweighed by the injuries suffered by Plaintiff and Class Members as a result of the Data Breach.

185. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members are at a current and ongoing risk of identity theft, and Plaintiff and Class Members sustained compensatory damages including: (i) invasion of privacy; (ii) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (iii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iv) financial "out of pocket" costs incurred due to actual identity theft; (v) loss of time incurred due to actual identity theft; (vi) loss of time due to increased spam and targeted marketing emails; (vii) diminution of value of their Private Information; (viii) future costs of identity theft monitoring; (ix) anxiety, annoyance and nuisance, and (x) the continued risk to their Private Information, which remains in Defendants' control, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

186. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

187. Defendants' negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner.

188. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and All Class Members Against Defendants PSC and PBI)

189. Plaintiff and the Class repeat and re-allege each and every allegation as if fully set forth herein.

190. Upon information and belief, PSC entered into contracts with its government and corporate customers to provide secure file transfer services to them; services that included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was entrusted to it.

191. Upon information and belief, PBI entered into contracts with its government and corporate customers to provide beneficiary search services; services that included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was entrusted to it.

192. Such contracts were made expressly for the benefit of Plaintiff and the Class, as it was their Private Information that Defendants agreed to receive, store, utilize, transfer, and protect through its services. Thus, the benefit of collection and protection of the Private Information

belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties and Plaintiff and Class Members were direct and express beneficiaries of such contracts.

193. Defendants knew or should have known that if it were to breach these contracts with its customers, Plaintiff and Class Members would be harmed.

194. Defendants breached their contracts with customers by, among other things, failing to adequately secure Plaintiff and Class Members' Private Information, and, as a result, Plaintiff and Class Members were harmed by Defendants' failure to secure their Private Information.

195. As a direct and proximate result of Defendants' breach, Plaintiff and Class Members are at a current and ongoing risk of identity theft, and Plaintiff and Class Members sustained incidental and consequential damages including: (i) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out of pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their Private Information; (vii) future costs of identity theft monitoring; (viii) and the continued risk to their Private Information, which remains in Defendants' control, and which is subject to further breaches, so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

196. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

197. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit

to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
BREACH OF CONTRACT
(On Behalf of Plaintiff and TIAA Subclass Members Against Defendant TIAA)

198. Plaintiff and the TIAA Subclass repeat and re-allege each and every allegation as if fully set forth herein.

199. Upon information and belief, TIAA entered into contracts with customers, agents, and businesses to provide insurance and annuity services; services that included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was entrusted to it.

200. Plaintiff and TIAA Subclass members were parties to such contracts, as it was their Private Information that TIAA agreed to receive, store, utilize, transfer, and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties.

201. TIAA knew or should have known that if it were to breach these contracts with its customers, Plaintiff and TIAA Subclass Members would be harmed.

202. TIAA breached their contracts with customers by, among other things, failing to adequately secure Plaintiff and TIAA Subclass Members' Private Information, and, as a result, Plaintiff and TIAA Subclass Members were harmed by TIAA's failure to secure their Private Information.

203. As a direct and proximate result of TIAA's breach, Plaintiff and TIAA Subclass Members are at a current and ongoing risk of identity theft, and Plaintiff and TIAA Subclass Members sustained incidental and consequential damages including: (i) financial "out of pocket"

costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out of pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their Private Information; (vii) future costs of identity theft monitoring; (viii) and the continued risk to their Private Information, which remains in TIAA's control, and which is subject to further breaches, so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and TIAA Subclass Members' Private Information.

204. Plaintiff and TIAA Subclass Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

205. Plaintiff and TIAA Subclass Members are also entitled to injunctive relief requiring TIAA to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT IV
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and All Class Members Against All Defendants)

206. Plaintiff and the Class repeat and re-allege each and every allegation as if fully set forth herein.

207. Pursuant to Federal Trade Commission, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

208. Defendants breached their duties to Plaintiff and Class Members under the FTC

Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

209. Defendants' failure to comply with applicable laws and regulations constitutes negligence per se.

210. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

211. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that it was failing to meet its duties, and that Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

212. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members are at a current and ongoing risk of identity theft, and Plaintiff and Class Members sustained compensatory damages including: (i) invasion of privacy; (ii) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (iii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iv) financial "out of pocket" costs incurred due to actual identity theft; (v) loss of time incurred due to actual identity theft; (vi) loss of time due to increased spam and targeted marketing emails; (vii) diminution of value of their Private Information; (viii) future costs of identity theft monitoring; (ix) anxiety, annoyance and nuisance, and (x) the continued risk to their Private Information, which remains in Defendants' control, and which is subject to further breaches, so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

213. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

214. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiff and All Class Members Against All Defendants)

215. Plaintiff and the Class repeat and re-allege each and every allegation as if fully set forth herein.

216. Plaintiff and Class Members conferred a monetary benefit on Defendants by providing Defendants with their valuable Private Information.

217. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information, which cost savings increased the profitability of the services.

218. Upon information and belief, instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

219. Under the principles of equity and good conscience, Defendants should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that

are mandated by industry standards.

220. Defendants acquired the monetary benefit, PII, through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

221. Had Plaintiff and Class Members known that Defendants had not secured their PII, they would not have agreed to provide their PII to Defendants. Plaintiff and Class Members have no adequate remedy at law.

222. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

223. Furthermore, as a direct and proximate result of Defendants' unreasonable and inadequate data security practices, Plaintiff and Class Members are at a current and ongoing risk of identity theft and have sustained incidental and consequential damages, including: (i) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out of pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their Private Information; (vii) future costs of identity theft monitoring; and (viii) the continued risk to their Private Information, which remains in Defendants' control, and which is subject to further breaches, so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

224. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

225. Plaintiff and Class Members are also entitled to injunctive relief requiring

Defendants to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

226. Moreover, Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendants' services.

COUNT VI
DECLARATORY AND INJUNCTIVE RELIEF

227. Plaintiff and the Class repeat and re-allege each and every allegation as if fully set forth herein.

228. Plaintiff pursues this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

229. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

230. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class Members' Private Information, and whether Defendants is currently maintaining data security measures adequate to protect Plaintiff and Class Members from future data breaches that compromise their Private Information. Plaintiff and the Class remain at imminent risk that further compromises of their Private Information will occur in the future.

231. The Court should also issue prospective injunctive relief requiring Defendants to

employ adequate security practices consistent with law and industry standards to protect Plaintiff's and Class Members' Private Information.

232. Defendants still controls the Private Information of Plaintiff and the Class Members.

233. To Plaintiff's knowledge, Defendants has made no announcement that it has changed its data or security practices relating to the Private Information.

234. To Plaintiff's knowledge, Defendants has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

235. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at PSC. The risk of another such breach is real, immediate, and substantial.

236. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class members are at risk of additional or further harm due to the exposure of their Private Information and Defendants' failure to address the security failings that led to such exposure.

237. There is no reason to believe that Defendants' employee training and security measures are any more adequate now than they were before the breach to meet Defendants' contractual obligations and legal duties.

238. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if another data breach occurs at PSC, Plaintiff and Class Members will likely continue to be subjected to fraud, identify

theft, and other harms described herein. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants has a pre-existing legal obligation to employ such measures.

239. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach PSC, thus eliminating the additional injuries that would result to Plaintiff and Class.

240. Plaintiff and Class Members seek a declaration (i) that Defendants' existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security; and (ii) that to comply with its contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to, the following:

a. engage internal security personnel to conduct testing, including audits on Defendants' systems, on a periodic basis, and promptly correct any problems or issues detected by such third-party security auditors;

b. engage third-party security auditors and internal personnel to run automated security monitoring;

c. audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

d. purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for its provision of services;

e. conduct regular database scanning and security checks; and

f. routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, PII.

COUNT VII
VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW § 349
(On Behalf of Plaintiff and TIAA Subclass Members Against Defendant TIAA)

241. Plaintiff and the TIAA Subclass repeat and re-allege each and every allegation as

if fully set forth herein.

242. New York General Business Law Section 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

243. TIAA ("Defendant" for purposes of this Count) is a business subject to N.Y. Gen. Bus. Law § 349.

244. Plaintiff and TIAA Subclass Members are consumers as defined by the statute.

245. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of New York Gen. Bus. Law § 349. The conduct alleged is a "business practice" as defined by the statute, and the deception occurred in New York state.

246. Defendant engaged in deceptive acts or practices in the conduct of business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and TIAA Subclass Members' PII, which was a proximate and direct cause of the Data Breach; failing to identify foreseeable security and privacy risks in both its own and its third-party vendors' technology systems, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents involving other organizations, which was a direct and proximate cause of the Data Breach; misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and TIAA Subclass Members' PII, including by implementing and maintaining reasonable security measures at both its own and its third-party vendors' technology systems; failing to timely and adequately notify Plaintiff and TIAA Subclass Members of the Data Breach; failing to oversee and monito third-party vendors responsible for the storage and transfer of PII; omitting, suppressing, and concealing the material

fact that it did not reasonably or adequately secure Plaintiff's and TIAA Subclass Members' PII; and omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and TIAA Subclass Members' PII.

247. Defendant's representations and omissions regarding data security were material because they were about the critical need and adequacy of Defendant's data security and ability to protect the confidentiality of PII.

248. Defendant acted intentionally and knowingly to violate New York's General Business Law, and recklessly disregarded Plaintiff's and TIAA Subclass Members' rights.

249. As a direct result of Defendant's deceptive and unlawful acts and practices, Plaintiff and TIAA Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; and increased, imminent risk of fraud and identity theft; loss of value of their PII; an increased, imminent risk of fraud and identity theft; loss of value of the PII; and the other harms discussed herein.

250. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large. Defendant's violations of the statute have had an impact on the public, including the people of New York.

251. The above deceptive and unlawful practices and acts by Defendant caused substantial injury to Plaintiff and TIAA Subclass members that they could not reasonably avoid.

252. As such, Plaintiff and the TIAA Subclass members seek statutory damages in the maximum amount allowed per Subclass member, or, $50 for each victim of the Data Breach.

Additionally, Plaintiff and the TIAA Subclass members seek injunctive relief necessary to enjoin further violations and recover costs of this action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendants and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and their Counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

viii. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

ix. requiring Defendants to conduct regular database scanning and securing checks;

x. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and

to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: September 1, 2023

Respectfully Submitted,

/s/ Jeffrey Brown

Jeffrey Brown*
LEEDS BROWN LAW
One Old Country Road, Suite 347
Carle Place, NY 11514-1851
JBrown@LeedsBrownLaw.com

Jason P. Sultzer*
THE SULTZER LAW GROUP P.C.
85 Civic Center Plaza, Suite 200
Poughkeepsie, NY 12601
Phone: (845) 244-5595
sultzerj@thesultzerlawgroup.com

Steve W. Berman*
Sean R. Matt*
HAGENS BERMAN SOBOL SHAPIRO
1301 Second Avenue, Suite 2000
Seattle, WA 98101
Phone: (206) 623-7292
Fax: (206) 623-0594
steve@hbsslaw.com
sean@hbsslaw.com

Jeffrey S. Goldenberg*
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
Phone: (513) 345-8291
Fax: (513) 345-8294
jgoldenberg@gs-legal.com

Charles Schaffer*
Nicholas J. Elia*
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Phone: (215) 592-1500
Fax: (215) 592-4663
cschaffer@lfsblaw.com
nelia@lfsblaw.com

Joseph M. Lyon*
THE LYON FIRM
2754 Erie Ave.
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

**Pro Hac Vice Application forthcoming*

Counsel for Plaintiff and the Putative Class